NATIONAL INSTITUTE OF TECHNOLOGY PATNA

Department of Computer Science and Engineering

Mid Semester Exam 2022

Subject: Blockchain Technology (CS6475)

Full Marks: 30 **Duration: 2 Hours**

All questions are compulsory. Make assumption of missing data if any.
Please write precise and to the point answers, irrelevant and lengthy answers may attract penalty.

1. Let H be a hash function that is both hiding and puzzle-friendly. Consider G(z) = H(z) | z_{last} where z_{last} represents the last bit of z. Show that G is puzzle-friendly but not hiding. Define any cryptographic hashing algorithm. [6]

2. If a malicious ISP completely controls a user's connections, can it launch a double-spend attack against the user? How much computational effort would this take? Assuming that the total hash power of the network stays constant, what is the probability that a block will be found in the next 10 minutes? [6]

3. Suppose Bob the merchant wants to have a policy that orders will ship within *x* minutes after receipt of payment. What value of *x* should Bob choose so that with 99% confidence 6 blocks will be found within *x* minutes? [6]

4.i) Compare and contrast attacks on digital signatures with attacks on cryptosystems.
ii) Using the RSA scheme, let p= 809, q = 751 and d=23. Calculate the public key e.
a) Sign and verify a message with M1 = 100. Call the signature S1.
b) Sign and verify a message with M2 = 50. Call the signature S2.
c) Show that if M = M1*M2 = 5000, then S = S1*S2. [6]

5. Write a function explaining different operations (add element, get element, update element) used in array in Solidity. [6]